Claims

1. A financial transaction verification system comprising:

a transaction processing client;

a transaction processing server under the control of a financial services provider;

a programmable telecommunications client under the control of a transaction initiator;

the transaction processing client, the transaction processing server and the telecommunications client all being connected to or adapted for connection to a telecommunications network;

the transaction processing client being adapted, when in use a transaction is initiated and processed through the transaction processing client, to record:

data pertaining to a transaction initiated, in use, by the transaction initiator; and

data pertaining to a financial account of the transaction initiator with the financial services provider;

the transaction processing client being adapted to transmit the recorded data to the transaction processing server by way of the telecommunications network;

the transaction processing server being adapted to make use of data pertaining to the transaction initiator and the telecommunications client previously stored with the financial services provider to formulate a transaction authorisation request to the telecommunications client;

the transaction processing server being adapted to transmit the transaction authorisation request to the telecommunications client by way of the telecommunications network;

the telecommunications client being programmed to require the entry of an authorisation code into the telecommunications client as a precondition for the

further processing of the transaction authorisation request; and

the telecommunications client being programmed, further, to transmit a process outcome message to either or both the transaction processing server and the transaction processing client, which process outcome message:

if the incorrect authorisation code is entered, is constituted by a transaction cancellation signal; and

if the correct authorisation code is entered, is constituted by a transaction authorisation signal.

2. A financial transaction verification system according to claim 1 in which the telecommunications client is a mobile communication device that is personal to the transaction initiator, in which system:

the transaction initiator data previously stored with the financial services provider includes unique mobile communication device data, which is data that is unique to and stored in the mobile communication device;

the transaction processing server is adapted to transmit the previously stored unique mobile communication device data to the mobile communication device together with the authorisation request;

the mobile communication device is programmed, on receipt of the transmitted data, to compare the transmitted data to the equivalent unique mobile communication device data stored in the mobile communication device;

the telecommunications client is programmed, further, to transmit a process outcome message to either or both the transaction processing server and the transaction processing client, which process outcome message may, alternatively, be constituted by a transaction cancellation signal or a transaction authorisation signal;

the mobile communication device being programmed, further:

if the comparison between the transmitted data and the equivalent data stored in the mobile communication device fails, to transmit a process

outcome message constituted by a transaction cancellation signal; and

if the comparison is successful, to require the entry, into the mobile communication device, of the authorisation code previously provided as a precondition for the further processing of the transaction authorisation request; and

if the incorrect authorisation code is entered, to transmit a process outcome message constituted by a transaction cancellation signal; and

if the correct authorisation code is entered to transmit a process outcome message constituted by a transaction authorisation signal.

3. A financial transaction verification system according to either of the preceding claims that is adapted:

to cancel the transaction in the event of the receipt, by the telecommunications client, of a transaction cancellation signal; and

to allow the transaction to proceed to finality in the event of the receipt, by the telecommunications client, of a transaction authorisation signal.

4. A transaction processing client for use with a system according to any one of the preceding claims.

5. A transaction processing server for use with a system according to any one of the preceding claims.

6. A telecommunications server for use with a system according to any one of the preceding claims.

7. A telecommunications client for use with a system according to any one of the preceding claims.

8. A method of verifying a financial transaction comprising the steps of:

initiating a transaction at a transaction processing client;

recording, by means of the transaction processing client, data pertaining to the transaction together with data pertaining to a financial account of the transaction initiator with a financial services provider;

transmitting the data so recorded from the transaction processing client to a transaction processing server under control of the financial services provider, by way of a telecommunications network,

supplying, to the transaction processing server, data previously stored with the financial services provider and pertaining to a telecommunications client which is under the control of the transaction initiator;

transmitting an authorisation request pertaining to the initiated transaction to the telecommunications client;

requiring, on receipt of such a transaction authorisation request, the entry into the telecommunications client, of an authorisation code as a precondition for the further processing of the transaction authorisation request;

transmitting a process outcome message to either or both the transaction processing server and the transaction processing client, which process outcome message:

if the incorrect authorisation code is entered, is constituted by a transaction cancellation signal; and

if the correct authorisation code is entered, is constituted by a transaction authorisation signal.

9. A method of verifying a financial transaction according to claim 8 in which the telecommunications client is a mobile communication device personal to the transaction initiator and data unique to and stored in the mobile communication device is stored by the financial services provider as part of the communications data pertaining to the transaction initiator, the method including the additional steps of:

transmitting the unique mobile communication device data from the transaction processing server to the mobile communication device together with the authorisation request;

in the mobile communication device, comparing, on receipt of the transmitted data and authorisation request, the transmitted unique mobile communication device data to the equivalent mobile communication device data stored in the mobile communication device; and

if the comparison between the transmitted data and the equivalent data stored in the mobile communication device fails, transmitting a transaction cancellation signal to either or both the transaction processing server and the transaction processing client; and

if the comparison is successful, requiring the entry of the authorisation code previously provided into the mobile communication device as a precondition for the further processing of the transaction authorisation request; and

if the incorrect authorisation code is entered, transmitting a transaction cancellation signal to either or both the transaction processing server and the transaction processing client; and

if the correct code is entered, transmitting a transaction authorisation signal to either or both the transaction processing server and the transaction processing client.

10. A method of verifying a financial transaction according to either of claims 8 or 9 which includes the additional steps of:

canceling the transaction in the event of the receipt, by the telecommunications client, of a transaction cancellation signal; and

allowing the transaction to proceed to finality in the event of the receipt, by the telecommunications client, of a transaction authorisation signal.

11. A method of verifying a financial transaction according to claim 8 in which the transaction involves the use of a documentary negotiable instrument, the method comprising the steps of:

initiating the transaction by a participating negotiable instrument issuer issuing the negotiable instrument manually;

recording, by means of the transaction processing client, data pertaining to the transaction including predetermined data pertaining to the negotiable instrument;

transmitting the data so recorded from the transaction processing client to the transaction processing server by way of the telecommunications network,

transmitting, to either or both the financial services provider and the transaction processing server, a negotiable instrument issuer code unique to the negotiable instrument issuer, thereby to confirm, to the transaction processing server, the transmitted data pertaining to the transaction including the predetermined data pertaining to the negotiable instrument;

recording, at the transaction processing server, the data so confirmed; and

comparing, when in use the negotiable instrument is presented for payment, the data on the face of the documentary negotiable instrument with the data recorded in the transaction processing server in respect of that negotiable instrument.

12. A method of operating a transaction processing server for use in a financial transaction verification method according to claim 11, the method comprising the steps of:

receiving the entry of data pertaining to negotiable instruments from participating negotiable instrument issuers;

receiving, from each participating negotiable instrument issuer and in respect of the data pertaining to each such negotiable instrument, a unique negotiable instrument issuer code;

confirming the validity of each negotiable instrument issuer code so entered by comparing the negotiable instrument issuer code so entered with a negotiable instrument issuer code stored in the transaction processing server; and

permitting a participating presentation point to gain access to the data stored in respect of a particular negotiable instrument when that negotiable instrument is presented for payment, thereby to allow comparison between the stored data and the data appearing on the face of the negotiable instrument.

13. A method of verifying a financial transaction according to claim 8 in which the transaction involves the use of a communications enabled transaction terminal as the transaction processing client, the method including the steps of:

with the use of the mobile communication device, formulating and encrypting, by means of a first encryption key and data unique to the mobile communication device, a transaction request to be transmitted to the transaction terminal and

transmitting a transaction request directly to the transaction terminal with the use of the mobile communication device, using a method of communication for which the transaction terminal is enabled;

transmitting the transaction request from the transaction terminal to the transaction processing server;

at the transaction processing server:

receiving the transaction request;

identifying the mobile communication device using the data unique to the mobile communication device;

retrieving the first encryption key, previously stored at the transaction processing server in respect of the mobile communication device;

decrypting the encrypted transaction request using the first encryption key;

processing the transaction request and generating a process outcome message pertaining to the result of processing of the transaction request;

generating a second encryption key, storing the second encryption key in the transaction processing server;

transmitting the second encryption key to the transaction terminal;

encrypting the process outcome message using the second encryption key; and

transmitting the encrypted process outcome message to the mobile communication device;

at the mobile communication device, extracting and storing the second encryption key and transmitting the encrypted process outcome message to the transaction terminal; and

at the transaction terminal, decrypting the encrypted process outcome message and applying the decrypted process outcome message to actuate the transaction terminal.

14. A method of verifying a financial transaction according to claim 13 in which the second encryption key that is stored at the transaction processing server and in the mobile communication device is used, in a following transaction processing cycle as the first encryption key.

15. A method of verifying a financial transaction according to claim 14 in which the second encryption key is generated, every time the transaction processing cycle is repeated, with the use of code hopping techniques.

16. A method of verifying a financial transaction according to any one of claims 13 to 15 in which, in the process of encrypting the transaction request to be transmitted to the transaction processing server, the transaction request is encrypted with the use, in addition, of a code unique to the person requesting the transaction.